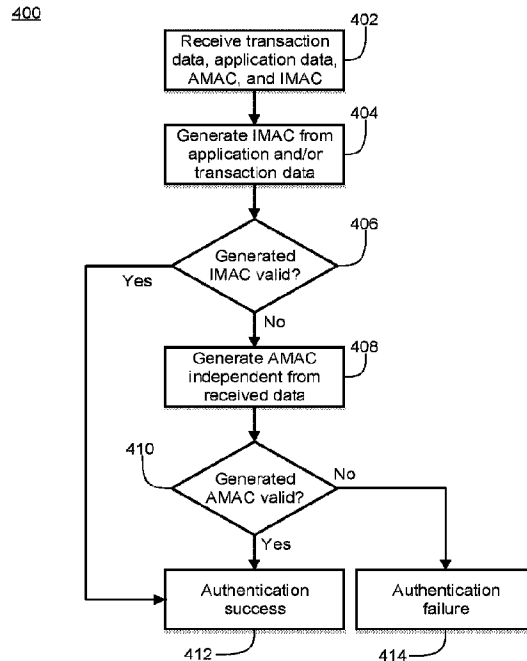




(86) **Date de dépôt PCT/PCT Filing Date:** 2016/07/01
 (87) **Date publication PCT/PCT Publication Date:** 2018/01/04
 (45) **Date de délivrance/Issue Date:** 2022/12/06
 (85) **Entrée phase nationale/National Entry:** 2018/12/31
 (86) **N° demande PCT/PCT Application No.:** US 2016/040803
 (87) **N° publication PCT/PCT Publication No.:** 2018/004679

(51) **Cl.Int./Int.Cl. H04L 9/32** (2006.01),
G06Q 20/32 (2012.01), **G06Q 20/40** (2012.01)
 (72) **Inventeurs/Inventors:**
SILVESTRE, CARLOS EDUARDO OLIVEIRA DO
VALLE, GB;
LUPTON, JONATHAN WARD, GB
 (73) **Propriétaire/Owner:**
AMERICAN EXPRESS TRAVEL RELATED SERVICES
COMPANY, INC., US
 (74) **Agent:** MARKS & CLERK

(54) **Titre : SYSTEMES ET PROCEDES DE VALIDATION DE TRANSMISSIONS SUR DES CANAUX DE COMMUNICATION**
 (54) **Title: SYSTEMS AND METHODS FOR VALIDATING TRANSMISSIONS OVER COMMUNICATION CHANNELS**



(57) **Abrégé/Abstract:**

An authentication system may receive an authentication MAC, an integrity MAC, and data transmitted from a payment application and a payment terminal. A local integrity MAC may be generated using the data as an input to a first cryptographic operation. The system may compare the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC. A local authentication MAC may be generated using a second cryptographic operation and compare the local authentication MAC to the received authentication MAC. The system may authenticate the payment application in response to a successful authentication of at least one of the received authentication MAC or the received integrity MAC.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(10) International Publication Number
WO 2018/004679 A1

(43) International Publication Date
04 January 2018 (04.01.2018)

(51) International Patent Classification:

H04L 9/32 (2006.01) G06Q 20/40 (2012.01)
G06Q 20/32 (2012.01)

(21) International Application Number:

PCT/US2016/040803

(22) International Filing Date:

01 July 2016 (01.07.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC. [US/US]; 200 Vesey Street, 3 World Financial Center, New York, NY 10285-4900 (US).

(72) Inventors: SILVESTRE, Carlos Eduardo Oliveira Do Valle; 14 Charles Close Hove, East Sussex BN3 6WP (GB). LUPTON, Jonathan Ward; 35 Nursery Road, Angmering, Littlehampton, West Sussex BN16 4GQ (GB).

(74) Agent: KIRBY, Nicholas; Snell & Wilmer LLP, One Arizona Center, 400 E. Van Buren, Phoenix, AZ 85004 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ,

EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

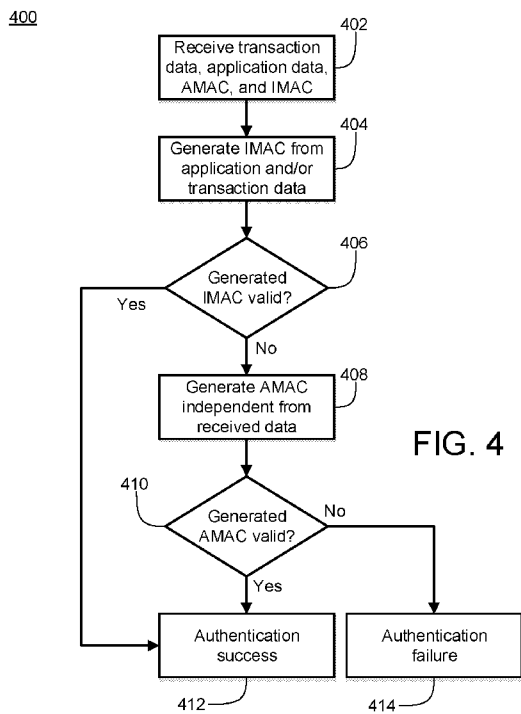
Published:

- with international search report (Art. 21(3))
- with amended claims (Art. 19(1))



WO 2018/004679 A1

(54) Title: SYSTEMS AND METHODS FOR VALIDATING TRANSMISSIONS OVER COMMUNICATION CHANNELS



(57) Abstract: An authentication system may receive an authentication MAC, an integrity MAC, and data transmitted from a payment application and a payment terminal. A local integrity MAC may be generated using the data as an input to a first cryptographic operation. The system may compare the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC. A local authentication MAC may be generated using a second cryptographic operation and compare the local authentication MAC to the received authentication MAC. The system may authenticate the payment application in response to a successful authentication of at least one of the received authentication MAC or the received integrity MAC.

TITLE: SYSTEMS AND METHODS FOR VALIDATING
TRANSMISSIONS OVER COMMUNICATION CHANNELS

5

FIELD

[0001] This disclosure relates to systems and methods for validating payment data transmitted in order to complete payment transactions.

10

BACKGROUND

[0002] Electronic payment transactions may be processed by transmitting data from a payment terminal to an authentication host. During transmission, the data may be corrupted due to faults in the payment network. As a result, the authentication host may not receive the expected data and the payment transaction may not be approved as the authentication host may not be capable of validating payment data due to the corrupted data.

15

[0003] Electronic payment transactions may also be targeted for fraudulent transactions. In some instances, fraudulent transactions are detected during authentication by the same authentication failures resulting from a network error. An authentication failure may be the result of fraud, and an authentication failure may also be the result of a network error. However, the authentication systems may be unable to distinguish between network errors and fraudulent transactions.

20

[0004] After authentication failure, the payment network may decide whether to allow the transaction. Despite authentication failure, a transaction with a low fraud risk may still be approved. For example, the payment network may determine that the requested transaction amount is low enough to authorize, despite of the failure. As a result, fraudulent transactions may be authorized in some instances.

25

SUMMARY

[0005] A system, method, and/or computer readable medium (collectively, the "system") is disclosed for authenticating a payment application and payment data involved in a payment transaction. The system receives an authentication Message Authentication Code (MAC), an integrity MAC, and data transmitted from a payment application. A local integrity MAC may be generated using the data as an input to a first cryptographic operation. The system may

30

compare the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC. A local authentication MAC may be generated using a second cryptographic operation and the local authentication MAC may be compared to the received authentication MAC. The system may authenticate the payment application in response to a successful authentication of at least one of the received authentication MAC or the received integrity MAC.

[0006] In various embodiments, the system may retrieve an input to the second cryptographic operation that is generated independently from the data used as the input to the first cryptographic operation. In that regard, the input to the authentication MAC may be independent from data transmission failures. The input to the second cryptographic operation may include a date or a transaction counter, for example. The first cryptographic operation may be the same as the second cryptographic operation and may comprise an authentication encryption mode. A transaction may be approved in response to the successful authentication of at least one of the authentication MAC or the integrity MAC. The authentication MAC, the integrity MAC and payment application data may be transmitted from the payment application to a payment terminal. The payment terminal sends, through a payment network and to the processor, all data received from the payment application and other relevant payment terminal transaction data.

According to an aspect of the present invention there is provided a method comprising:

receiving, by a processor, an authentication MAC, an integrity MAC, and transaction data transmitted from a payment application and a payment terminal, wherein the integrity MAC is generated from the transaction data using a cryptography key stored in the payment application;

generating, by the processor, a local integrity MAC using the transaction data as an input to a first cryptographic operation using a copy of the cryptography key accessible by the processor;

determining, by the processor, that the received integrity MAC fails to match the local integrity MAC by comparing the local integrity MAC to the received integrity MAC;

retrieving, by the processor, an input to a second cryptographic operation, wherein the input to the second cryptographic operation is generated independently from the transaction data received by the processor from the payment application and the payment terminal;

generating, by the processor, a local authentication MAC using the second cryptographic operation;

in response to the received integrity MAC failing to match the local integrity MAC, authenticating, by the processor, the received authentication MAC by comparing, by the processor, the local authentication MAC to the received authentication MAC; and

in response to authenticating the received authentication MAC, authenticating, by the processor, the payment application.

According to another aspect of the present invention there is provided a computer-based system comprising:

a processor;

a tangible, non-transitory memory configured to communicate with the processor, the tangible, non-transitory memory having instructions stored thereon that, in response to execution by the processor, cause the processor to perform operations comprising:

receiving, by the processor, an authentication MAC, an integrity MAC, and transaction data transmitted from a payment application and a payment terminal, wherein the integrity MAC is generated from the transaction data using a cryptography key stored in the payment application;

generating, by the processor, a local integrity MAC using the transaction data as an input to a first cryptographic operation using a copy of the cryptography key accessible by the processor;

determining, by the processor, that the received integrity MAC fails to match the local integrity MAC by comparing, by the processor, the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC;

retrieving, by the processor, an input to a second cryptographic operation, wherein the input to the second cryptographic operation is generated independently from the transaction data received by the processor from the payment application and the payment terminal;

generating, by the processor, a local authentication MAC using the second cryptographic operation;

in response to the received integrity MAC failing to match the local integrity MAC, authenticating, by the processor, the received authentication MAC by comparing, by the processor, the local authentication MAC to the received authentication MAC to authenticate the received authentication MAC; and

in response to authenticating the received authentication MAC, authenticating, by the processor, the payment application in response to a successful authentication of at least one of the received authentication MAC or the received integrity MAC.

According to a further aspect of the present invention there is provided an article of manufacture including a non-transitory, tangible computer readable storage medium having instructions stored thereon that, in response to execution by a processor, cause the processor to perform operations comprising:

receiving, by the processor, an authentication MAC, an integrity MAC, and transaction data transmitted from a payment application and a payment terminal, wherein the integrity MAC is generated from the transaction data using a cryptography key stored in the payment application;

generating, by the processor, a local integrity MAC using the transaction data as an input to a first cryptographic operation using a copy of the cryptography key accessible by the processor;

determining, by the processor, that the received integrity MAC fails to match the local integrity MAC by comparing, by the processor, the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC;

retrieving, by the processor, an input to a second cryptographic operation, wherein the input to the second cryptographic operation is generated independently from the transaction

data received by the processor from the payment application and the payment terminal;
generating, by the processor, a local authentication MAC using the second
cryptographic operation;

in response to the received integrity MAC failing to match the local integrity MAC,
authenticating, by the processor, the received authentication MAC by comparing, by the
processor, the local authentication MAC to the received authentication MAC to
authenticate the received authentication MAC; and

in response to authenticating the received authentication MAC, authenticating, by the
processor, the payment application in response to a successful authentication of at least
one of the received authentication MAC or the received integrity MAC.

[0007] The forgoing features and elements may be combined in various combinations
without exclusivity, unless expressly indicated herein otherwise. These features and elements
as well as the operation of the disclosed embodiments will become more apparent in light of
the following description and accompanying drawings.

BRIEF DESCRIPTION

[0008] The subject matter of the present disclosure is particularly pointed out and
distinctly claimed in the concluding portion of the specification. A more complete
understanding of the present disclosure, however, may be obtained by referring to the detailed
description and claims when considered in connection with the drawing figures, wherein like
numerals denote like elements.

[0009] FIG. 1 illustrates an exemplary system for authenticating and validating
payment transactions, in accordance with various embodiments;

[0010] FIG. 2 illustrates an exemplary process for the exchange and validation of
authentication data for payment transactions, in accordance with various embodiments;

[0011] FIG. 3 illustrates an exemplary process for execution by a payment application to generate authentication data for validation, in accordance with various embodiments; and

[0012] FIG. 4 illustrates an exemplary process for execution by an authenticating system to validate a transmission from a payment application, in accordance with various
5 embodiments.

DETAILED DESCRIPTION

[0013] The detailed description of various embodiments herein makes reference to the accompanying drawings and pictures, which show various embodiments by way of
10 illustration. While these various embodiments are described in sufficient detail to enable those skilled in the art to practice the disclosure, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the disclosure. Thus, the detailed description herein is presented for purposes of illustration only and not of limitation. For example, the steps
15 recited in any of the method or process descriptions may be executed in any order and are not limited to the order presented. Moreover, any of the functions or steps may be outsourced to or performed by one or more third parties. Furthermore, any reference to singular includes plural embodiments, and any reference to more than one component may include a singular embodiment.

[0014] The disclosure includes peripherals, devices, systems and networks for validating a payment transaction. A portable device containing a payment application interacts with a payment terminal to perform a payment transaction that may be authorized by an issuer host. The payment application may have a protected Authentication Symmetric Cryptography Key (ASCK). During the payment transaction, the payment application may use the ASCK to
25 compute two Message Authentication Codes (MACs). The first MAC may be computed using as input the payment transaction data, such as transaction amount, date and terminal transaction information, combined with payment application data, such as a payment application transaction counter. The second MAC may be computed using as input any data that can be replicated in the issuer host, regardless of the network message. Both MACs are
30 transmitted to issuer host through the payment network. The issuer host may authenticate the payment application and/or the transaction data separately by validating one or both MACs independently.

[0015] With reference to FIG. 1, system 100 for completing electronic transactions is shown, in accordance with various embodiments. System 100 facilitates transactions between payment application 102 and point-of-sale (POS) terminal 104. Payment application 102 may be a device capable of performing cryptographic operations and configured to generate two MACs for each transaction. Thus, as described in greater detail herein, a MAC may be an output of a cryptographic function or operation.

[0016] A payment application 102 may include a computing device having a processor and memory such as, for example, a computer or set of computers. A payment application 102 may also include other types of computing units or systems such as laptops, notebooks, tablets, hand held computers, personal digital assistants, set-top boxes, workstations, servers, mainframe computers, mini-computers, pervasive computers, network sets of computers, personal computers, kiosks, terminals, televisions, or any other device capable of generating and communicating MACs. Payment application 102 may also include chip cards with a chip configured to generate MACs for authentication.

[0017] Payment application 102 may include a software application installed on a computing device or a chip having cryptographic capabilities to generate MACs. The payment application may generate the MACs using an Authentication Symmetric Cryptographic Key (ASCK) to be used as an authentication mechanism. An issuer host 108 may store, or be capable of generating, the same ASCK used by payment application 102 to generate MACs and apply the same cryptographic operations. The cryptographic operations may be performed by way of any of the techniques now available in the art or which may become available such as, for example, 3DES, AES, Twofish, Serpent, Blowfish, CAST5, IDEA, or other suitable symmetric cryptographic operations. Cryptographic operations may also include authentication encryption modes as standardized in ISO/IEC 19772:2009 such as, for example, OCB 2.0, Key Wrap, CCM, EAX, Encrypt-then-MAC (EtM), and GCM. The cryptographic function may take an input including plain text and a key to generate cyphered text. The cryptographic function may be deterministic and/or one-to-one in nature such that the same cyphered text is always generated from the same input. A MAC may have a length of, for example, 4 bytes, 8 bytes, 16 bytes, 32 bytes, or another suitable length.

[0018] Payment application 102 may be associated with a transaction account. Transaction data and account data may include an account number or other account information. The account number may be distributed and stored in any form of plastic,

electronic, magnetic, radio frequency, wireless, audio and/or optical on payment application 102 capable of transmitting or downloading data from itself to a payment terminal 104.

5 [0019] In various embodiments, an account number may identify a consumer. In addition, in various embodiments, a consumer may be identified by a variety of identifiers, including, for example, an email address, a telephone number, a cookie id, a radio frequency identifier (RFID), a biometric, and the like.

[0020] The payment terminal 104 may include any of the computing devices discussed herein capable of communication with payment application 102. Payment terminal 104 may communicate with payment application 102 over communication channel 103.
10 Communication channel 103 may include a chip reader, a magnetic stripe reader, an NFC channel, a Bluetooth® channel, an optical communication channel, a local area network (LAN) connection, a wide area network connection (WAN), and/or another communication channel suitable for communicating a MAC from payment application 102 to payment terminal 104.

15 [0021] Payment terminal 104 may transmit two or more MACs for authentication through payment network 106 to issuer host 108. As used herein, “transmit” may include sending electronic data from one system component to another over a network connection. Payment network 106 may include a network of computing devices, as described herein, and communication channels. The MACs may be passed through payment network 106, where
20 transmission errors and/or processing errors may alter a MAC and/or transaction data prior to arrival at issuer host. Issuer host 108 may re-generate the MACs using available data and compare the re-generated MACs to those received from payment application 102, payment terminal 104, and/or payment network 106. Issuer host 108 may successfully authenticate in response to the re-generated MACs matching the received MACs. Issuer host 108 may fail to
25 authenticate in response to the re-generated MACs conflicting with the received MACs. The MACs described herein may be cryptograms resulting from cryptogram operations. Exemplary cryptogram operations include those documented in the EMV 4.3 specification, any transaction specification supported by EMVCo and specified at <http://www.emvco.com/specifications.aspx>.

30 [0022] As used herein, “satisfy”, “meet”, “match”, “associated with” or similar phrases may include an identical match, a partial match, meeting certain criteria, matching a subset of data, a correlation, satisfying certain criteria, a correspondence, an association, an algorithmic relationship and/or the like. Similarly, as used herein, “authenticate” or similar terms may

include an exact authentication, a partial authentication, authenticating a subset of data, a correspondence, satisfying certain criteria, an association, an algorithmic relationship and/or the like.

[0023] Referring now to FIG. 2, an exemplary process 200 for authenticating a payment transaction conducted on system 100 is shown, in accordance with various embodiments. Payment application 102 and payment terminal may initiate a payment transaction in which payment application 102 and the associated account is being used to purchase goods or services at payment terminal 104. Payment terminal 104 may transmit transaction data to payment application 102. Transaction data may include a date, a time, a transaction amount, payment terminal 104 data, the type of transaction, and any other data suitable for MAC generation and/or transaction decisioning. Payment terminal 104 data may include a device identifier, a merchant identifier, transaction status, or any other data associated with payment terminal 104.

[0024] Terms and phrases similar to “associate” and/or “associating” may include tagging, flagging, correlating, using a look-up table or any other method or system for indicating or creating a relationship between elements, such as, for example, (i) a transaction account and (ii) an item (e.g., offer, reward, discount) and/or digital channel. Moreover, the associating may occur at any point, in response to any suitable action, event, or period of time. The associating may occur at pre-determined intervals, periodic, randomly, once, more than once, or in response to a suitable request or action. Any of the information may be distributed and/or accessed via a software enabled link, wherein the link may be sent via an email, text, post, social network input and/or any other method known in the art.

[0025] Payment application 102 may generate an authentication MAC (AMAC) and an integrity MAC (IMAC) (Step 204). The AMAC and IMAC may each be generated by generated by applying a cryptographic operation to input data. The cryptographic operation may be the same or different for the AMAC and IMAC, provided that the cryptographic operation may be reproduced by the issuer host for comparison and validation. The cryptographic operation may be performed on input data that is also made available at a later time to replicate the AMAC and IMAC by applying the same cryptographic operations. For example, the IMAC may be generated by taking transaction data and account data as an input and applying a cryptographic operation. The AMAC may be generated by taking data that may be available for authentication independent of a transmission from payment application 102. For example, the AMAC may be generated by taking the transaction date and/or

transaction time as an input and applying a cryptographic operation. Date and/or time may be available to other entities for use in regenerating the AMAC independently of data transmitted by payment application 102.

5 [0026] The payment application 102 may communicate the AMAC and IMAC each to payment terminal 104 (Step 206). The AMAC and IMAC may be transmitted contemporaneously, for example, in the same authentication packet. In addition to the AMAC and IMAC, payment application 102 may also communicate (in an authentication packet, for example) any other data used as input to generate the IMAC that is stored on and/or generated by the payment application 102. In that regard, by the end of the
10 transaction, payment terminal 104 may have the data necessary for transmission to issuer host 108. Payment terminal 104 may transmit to payment network 106 transaction and/or account data, the AMAC, and the IMAC (Step 208). The transaction and/or account data, the AMAC, and the IMAC may be transmitted through payment network 106 to issuer host 108 (Step 210).

15 [0027] Issuer host 108 may receive the transaction and/or account data, the AMAC, and the IMAC. In order to validate the IMAC, issuer host 108 may generate a local IMAC by applying the same cryptographic steps to the same inputs expected to be used by payment application 102 in Step 204 to generate the IMAC. The local IMAC may be compared to the IMAC received from payment network 106 (and payment application 102). In response to
20 the received IMAC matching the local IMAC, the received IMAC is authenticated successfully. In response to the received IMAC differing from the local IMAC, the IMAC authentication fails.

[0028] The AMAC may be used as a secondary authentication tool in response to the IMAC authentication failing. The AMAC may also be used as a secondary authentication
25 tool in addition to the IMAC authentication regardless of the IMAC authentication outcome. In order to validate the AMAC, issuer host 108 may generate a local AMAC by applying the same cryptographic steps to the same inputs expected to be used by payment application 102 in Step 204 to generate the AMAC. The local AMAC may be compared to the AMAC received from payment network 106 (and payment application 102). In response to the
30 received AMAC matching the local AMAC, the received AMAC is authenticated successfully. In response to the received AMAC differing from the local AMAC, the AMAC authentication fails.

[0029] By using the IMAC validation and AMAC validation in tandem, issuer host 108 may authenticate payment application 102 despite authentication failure of one of the IMAC or AMAC by validating the other. Thus, network errors causing an authentication failure in one of the MACs may be detected and the transaction may be authorized. Issuer host 108
5 may also detect a fraudulent or compromised transaction in response to neither the IMAC nor the AMAC successfully authenticating.

[0030] Referring now to FIG. 3, an exemplary process 300 for AMAC and IMAC authentication is shown for execution by payment application 102 and/or payment terminal 104, in accordance with various embodiments. The process may begin with retrieving
10 transaction data and account data (Step 302). The account data may be stored locally on payment application 102 and may include, for example, an account number, a security code, and/or expiration date. Transaction data may be generated, retrieved, and/or stored on payment terminal 104. For example, payment terminal 104 may scan a product and generate transaction data including, for example, a date, time, merchant identifier, and/or transaction
15 amount.

[0031] In various embodiments, payment application 102 may generate an IMAC using the resulting transaction data and/or account data (Step 304). The IMAC may be generated, as described herein, by taking transaction data and/or account data as an input and applying a cryptographic operation. The cryptographic operation should be repeatable given an identical
20 input. In that regard, issuer host 108 may reproduce the same IMAC in response to identical transaction data and account data arriving over payment network 106. However, varying input may result in authentication failure since the IMAC generated by issuer host 108 will not match an IMAC generated by payment application 102, if differing input is used for the cryptographic operation.

[0032] In various embodiments, payment application 102 may generate an AMAC using an input that is partially or fully independent from account data and/or transaction data (Step 306). The AMAC may be generated, as described herein, by taking an input that may be available independent of transmitted transaction data and account data and applying a cryptographic function. For example, the input may include a date, a time, a transaction
25 counter, a purchase credential, and/or data stored on both payment application 102 and issuer host 108. The cryptographic function may be the same as the cryptographic function used to generate the IMAC. The cryptographic function used to generate the AMAC may also vary
30 from the cryptographic function used to generate the IMAC provided that the cryptographic

function used to generate the AMAC generates the same AMAC given the same inputs (i.e., the cryptographic functions are deterministic).

[0033] In various embodiments, payment application 102 may transmit the transaction data, the account data, the AMAC, and the IMAC. As described herein, the transmission may go through payment network 106 to issuer host 108. Issuer host 108 may regenerate the AMAC and IMAC using the appropriate inputs and cryptographic functions described herein. The regenerated AMAC and IMAC may be compared to the transmitted AMAC and IMAC, respectively, with a match resulting in successful authentication.

[0034] Referring now to FIG. 4, an exemplary process 400 for authenticating payment application 102 is shown, in accordance with various embodiments. Any authenticating entity may execute process 400 to authenticate payment application 102. For example, issuer host 108 may authenticate payment application 102 using process 400. In various embodiments, issuer host may receive transaction data, account data, AMAC, and IMAC (Step 402). The transaction data and/or payment application data may be received in a transmission from one or more of payment application 102, payment terminal 104, and/or payment network 106.

[0035] In various embodiments, issuer host 108 may generate an IMAC from account data and/or transaction data (Step 404). As described herein, account data and/or transaction data received from payment application 102 may be used as an input to a cryptographic operation. The cryptographic operation may result in a locally generated IMAC for comparison to the IMAC received in Step 402. In various embodiments, issuer host 108 may determine whether the generated IMAC is valid (Step 406). Issuer host may make the determination by comparing the generated IMAC from Step 404 to the IMAC received in step 402. If the IMACs match then the generated IMAC is valid, and authentication is successful (Step 412).

[0036] In various embodiments, issuer host 108 may generate an AMAC independently from data received (Step 408) in response to the IMACs not matching. The AMAC may be generated using input that does not contain data received in Step 402. That is, data used as input to generate the AMAC at issuer host 108 may be stored, generated, or otherwise retrieved by AMAC independently of the transmission received in Step 402. Independent data may include a date, time, transaction counter, or transaction credential stored or retrieved by issuer host 108. Thus, although transaction data includes a transaction date, for example, issuer host may regenerate the date upon receiving the transmission in Step 402 rather than

reading the transaction date from the transmission. The regenerated date may be used in generating the AMAC, as the regenerated date is independently generated by issuer host 108.

[0037] In various embodiments, issuer host 108 may determine whether the generated AMAC is valid (Step 410). Issuer host may make the determination by comparing the generated AMAC from Step 408 to the AMAC received in step 402. If the AMACs match then the generated AMAC is valid, and authentication is successful (Step 412). If the AMACs do not match then the generated AMAC is invalid, and authentication is a failure (Step 414). Issuer host may approve a transaction in response to authentication success with a heightened level of confidence that the transaction is not fraudulent. Issuer host may also decline a transaction in response to authentication failure with a heightened level of confidence that the transaction is fraudulent.

[0038] Authentication systems and methods of the present disclosure may result in fewer disputed transactions due to the improved accuracy and robustness of the multiple-MAC authentication technique. The systems may decrease the approval rate of fraudulent payment transactions due to the granular authentication being performed. As a result, authenticators may experience a reduced fraud risk and devote fewer internal resources to investigate fraudulent transactions.

[0039] In various embodiments, the system and method may include alerting a subscriber when their computer is offline. The system may include generating customized information and alerting a remote subscriber that the information can be accessed from their computer. The alerts are generated by filtering received information, building information alerts and formatting the alerts into data blocks based upon subscriber preference information. The data blocks are transmitted to the subscriber's wireless device which, when connected to the computer, causes the computer to auto-launch an application to display the information alert and provide access to more detailed information about the information alert. More particularly, the method may comprise providing a viewer application to a subscriber for installation on the remote subscriber computer; receiving information at a transmission server sent from a data source over the Internet, the transmission server comprising a microprocessor and a memory that stores the remote subscriber's preferences for information format, destination address, specified information, and transmission schedule, wherein the microprocessor filters the received information by comparing the received information to the specified information; generates an information alert from the filtered information that contains a name, a price and a universal resource locator (URL), which specifies the location

of the data source; formats the information alert into data blocks according to said information format; and transmits the formatted information alert over a wireless communication channel to a wireless device associated with a subscriber based upon the destination address and transmission schedule, wherein the alert activates the application to
5 cause the information alert to display on the remote subscriber computer and to enable connection via the URL to the data source over the Internet when the wireless device is locally connected to the remote subscriber computer and the remote subscriber computer comes online.

[0040] In various embodiments, the system and method may include a graphical user
10 interface for dynamically relocating/rescaling obscured textual information of an underlying window to become automatically viewable to the user. By permitting textual information to be dynamically relocated based on an overlap condition, the computer's ability to display information is improved. More particularly, the method for dynamically relocating textual information within an underlying window displayed in a graphical user interface may
15 comprise displaying a first window containing textual information in a first format within a graphical user interface on a computer screen; displaying a second window within the graphical user interface; constantly monitoring the boundaries of the first window and the second window to detect an overlap condition where the second window overlaps the first window such that the textual information in the first window is obscured from a user's view;
20 determining the textual information would not be completely viewable if relocated to an unobstructed portion of the first window; calculating a first measure of the area of the first window and a second measure of the area of the unobstructed portion of the first window; calculating a scaling factor which is proportional to the difference between the first measure and the second measure; scaling the textual information based upon the scaling factor;
25 automatically relocating the scaled textual information, by a processor, to the unobscured portion of the first window in a second format during an overlap condition so that the entire scaled textual information is viewable on the computer screen by the user; and automatically returning the relocated scaled textual information, by the processor, to the first format within the first window when the overlap condition no longer exists.

[0041] In various embodiments, the system may also include isolating and removing
30 malicious code from electronic messages (e.g., email) to prevent a computer from being compromised, for example by being infected with a computer virus. The system may scan electronic communications for malicious computer code and clean the electronic

communication before it may initiate malicious acts. The system operates by physically isolating a received electronic communication in a “quarantine” sector of the computer memory. A quarantine sector is a memory sector created by the computer’s operating system such that files stored in that sector are not permitted to act on files outside that sector. When

5 a communication containing malicious code is stored in the quarantine sector, the data contained within the communication is compared to malicious code-indicative patterns stored within a signature database. The presence of a particular malicious code-indicative pattern indicates the nature of the malicious code. The signature database further includes code markers that represent the beginning and end points of the malicious code. The malicious

10 code is then extracted from malicious code-containing communication. An extraction routine is run by a file parsing component of the processing unit. The file parsing routine performs the following operations: scan the communication for the identified beginning malicious code marker; flag each scanned byte between the beginning marker and the successive end malicious code marker; continue scanning until no further beginning malicious code marker

15 is found; and create a new data file by sequentially copying all non-flagged data bytes into the new file, which forms a sanitized communication file. The new, sanitized communication is transferred to a non-quarantine sector of the computer memory. Subsequently, all data on the quarantine sector is erased. More particularly, the system includes a method for protecting a computer from an electronic communication containing malicious code by

20 receiving an electronic communication containing malicious code in a computer with a memory having a boot sector, a quarantine sector and a non-quarantine sector; storing the communication in the quarantine sector of the memory of the computer, wherein the quarantine sector is isolated from the boot and the non-quarantine sector in the computer memory, where code in the quarantine sector is prevented from performing write actions on

25 other memory sectors; extracting, via file parsing, the malicious code from the electronic communication to create a sanitized electronic communication, wherein the extracting comprises scanning the communication for an identified beginning malicious code marker, flagging each scanned byte between the beginning marker and a successive end malicious code marker, continuing scanning until no further beginning malicious code marker is found,

30 and creating a new data file by sequentially copying all non-flagged data bytes into a new file that forms a sanitized communication file; transferring the sanitized electronic communication to the non-quarantine sector of the memory; and deleting all data remaining in the quarantine sector.

[0042] In various embodiments, the system may also address the problem of retaining control over customers during affiliate purchase transactions, using a system for co-marketing the “look and feel” of the host web page with the product-related content information of the advertising merchant’s web page. The system can be operated by a third-party outsource provider, who acts as a broker between multiple hosts and merchants. Prior to implementation, a host places links to a merchant’s webpage on the host’s web page. The links are associated with product-related content on the merchant’s web page. Additionally, the outsource provider system stores the “look and feel” information from each host’s web pages in a computer data store, which is coupled to a computer server. The “look and feel” information includes visually perceptible elements such as logos, colors, page layout, navigation system, frames, mouse-over effects or other elements that are consistent through some or all of each host’s respective web pages. A customer who clicks on an advertising link is not transported from the host web page to the merchant’s web page, but instead is re-directed to a composite web page that combines product information associated with the selected item and visually perceptible elements of the host web page. The outsource provider’s server responds by first identifying the host web page where the link has been selected and retrieving the corresponding stored “look and feel” information. The server constructs a composite web page using the retrieved “look and feel” information of the host web page, with the product-related content embedded within it, so that the composite web page is visually perceived by the customer as associated with the host web page. The server then transmits and presents this composite web page to the customer so that she effectively remains on the host web page to purchase the item without being redirected to the third party merchant affiliate. Because such composite pages are visually perceived by the customer as associated with the host web page, they give the customer the impression that she is viewing pages served by the host. Further, the customer is able to purchase the item without being redirected to the third party merchant affiliate, thus allowing the host to retain control over the customer. This system enables the host to receive the same advertising revenue streams as before but without the loss of visitor traffic and potential customers. More particularly, the system may be useful in an outsource provider serving web pages offering commercial opportunities. The computer store containing data, for each of a plurality of first web pages, defining a plurality of visually perceptible elements, which visually perceptible elements correspond to the plurality of first web pages; wherein each of the first web pages belongs to one of a plurality of web page owners; wherein each of the first web pages displays at least

one active link associated with a commerce object associated with a buying opportunity of a selected one of a plurality of merchants; and wherein the selected merchant, the outsource provider, and the owner of the first web page displaying the associated link are each third parties with respect to one other; a computer server at the outsource provider, which
5 computer server is coupled to the computer store and programmed to: receive from the web browser of a computer user a signal indicating activation of one of the links displayed by one of the first web pages; automatically identify as the source page the one of the first web pages on which the link has been activated; in response to identification of the source page, automatically retrieve the stored data corresponding to the source page; and using the data
10 retrieved, automatically generate and transmit to the web browser a second web page that displays: information associated with the commerce object associated with the link that has been activated, and the plurality of visually perceptible elements visually corresponding to the source page.

[0043] Systems, methods and computer program products are provided. In the detailed
15 description herein, references to “various embodiments”, “one embodiment”, “an embodiment”, “an example embodiment”, etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature,
20 structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described. After reading the description, it will be apparent to one skilled in the relevant art(s) how to implement the disclosure in alternative embodiments.

[0044] In various embodiments, the methods described herein are implemented using the
25 various particular machines described herein. The methods described herein may be implemented using the particular machines described herein, and those hereinafter developed, in any suitable combination, as would be appreciated immediately by one skilled in the art. Further, as is unambiguous from this disclosure, the methods described herein may result in
30 various transformations of certain articles.

[0045] For the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the

connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical system.

5 [0046] The various system components discussed herein may include one or more of the following: a host server or other computing systems including a processor for processing digital data; a memory coupled to the processor for storing digital data; an input digitizer coupled to the processor for inputting digital data; an application program stored in the memory and accessible by the processor for directing processing of digital data by the
10 processor; a display device coupled to the processor and memory for displaying information derived from digital data processed by the processor; and a plurality of databases. Various databases used herein may include: client data; merchant data; financial institution data; and/or like data useful in the operation of the system. As those skilled in the art will appreciate, user computer may include an operating system (e.g., WINDOWS®, OS2,
15 UNIX®, LINUX®, SOLARIS®, MacOS, etc.) as well as various conventional support software and drivers typically associated with computers.

[0047] The present system or any part(s) or function(s) thereof may be implemented using hardware, software or a combination thereof and may be implemented in one or more computer systems or other processing systems. However, the manipulations performed by
20 embodiments were often referred to in terms, such as matching or selecting, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein. Rather, the operations may be machine operations. Useful machines for performing the various embodiments include general purpose digital computers or similar devices.
25

[0048] In fact, in various embodiments, the embodiments are directed toward one or more computer systems capable of carrying out the functionality described herein. The computer system includes one or more processors, such as processor. The processor is connected to a communication infrastructure (e.g., a communications bus, cross-over bar, or network).
30 Various software embodiments are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement various embodiments using other computer systems and/or architectures. Computer system can include a display interface that forwards graphics, text, and other data

from the communication infrastructure (or from a frame buffer not shown) for display on a display unit.

[0049] Computer system also includes a main memory, such as for example random access memory (RAM), and may also include a secondary memory. The secondary memory
5 may include, for example, a hard disk drive and/or a removable storage drive, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive reads from and/or writes to a removable storage unit in a well-known manner. Removable storage unit represents a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive. As will be appreciated, the removable
10 storage unit includes a computer usable storage medium having stored therein computer software and/or data.

[0050] In various embodiments, secondary memory may include other similar devices for allowing computer programs or other instructions to be loaded into computer system. Such devices may include, for example, a removable storage unit and an interface. Examples of
15 such may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an erasable programmable read only memory (EPROM), or programmable read only memory (PROM)) and associated socket, and other removable storage units and interfaces, which allow software and data to be transferred from the removable storage unit to computer system.

[0051] Computer system may also include a communications interface. Communications interface allows software and data to be transferred between computer system and external devices. Examples of communications interface may include a modem, a network interface
20 (such as an Ethernet card), a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communications interface are in the form of signals which may be electronic, electromagnetic, and optical or other signals capable of being received by communications interface. These signals are provided to communications interface via a communications path
25 (e.g., channel). This channel carries signals and may be implemented using wire, cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, wireless and other communications channels.
30

[0052] The terms “computer program medium” and “computer usable medium” and “computer readable medium” are used to generally refer to media such as removable storage

drive and a hard disk installed in hard disk drive. These computer program products provide software to computer system.

5 [0053] Computer programs (also referred to as computer control logic) are stored in main memory and/or secondary memory. Computer programs may also be received via communications interface. Such computer programs, when executed, enable the computer system to perform the features as discussed herein. In particular, the computer programs, when executed, enable the processor to perform the features of various embodiments. Accordingly, such computer programs represent controllers of the computer system.

10 [0054] In various embodiments, software may be stored in a computer program product and loaded into computer system using removable storage drive, hard disk drive or communications interface. The control logic (software), when executed by the processor, causes the processor to perform the functions of various embodiments as described herein. In various embodiments, hardware components such as application specific integrated circuits (ASICs). Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

15 [0055] In various embodiments, components, modules, and/or engines of system 100 may be implemented as micro-applications or micro-apps. Micro-apps are typically deployed in the context of a mobile operating system, including for example, a WINDOWS® mobile operating system, an ANDROID® Operating System, APPLE® IOS®, a BLACKBERRY® operating system and the like. The micro-app may be configured to leverage the resources of the larger operating system and associated hardware via a set of predetermined rules which govern the operations of various operating systems and hardware resources. For example, where a micro-app desires to communicate with a device or network other than the mobile device or mobile operating system, the micro-app may leverage the communication protocol of the operating system and associated device hardware under the predetermined rules of the mobile operating system. Moreover, where the micro-app desires an input from a user, the micro-app may be configured to request a response from the operating system which monitors various hardware components and then communicates a detected input from the hardware to the micro-app.

20 [0056] As used herein, the term "network" includes any cloud, cloud computing system or electronic communications system or method which incorporates hardware and/or software components. Communication among the parties may be accomplished through any suitable communication channels, such as, for example, a telephone network, an extranet, an intranet,

Internet, point of interaction device (point of sale device, personal digital assistant (e.g., IPHONE®, BLACKBERRY®), cellular phone, kiosk, etc.), online communications, satellite communications, off-line communications, wireless communications, transponder communications, local area network (LAN), wide area network (WAN), virtual private network (VPN), networked or linked devices, keyboard, mouse and/or any suitable communication or data input modality. Moreover, although the system is frequently described herein as being implemented with TCP/IP communications protocols, the system may also be implemented using IPX, APPLE®talk, IP-6, NetBIOS®, OSI, any tunneling protocol (e.g. IPsec, SSH), or any number of existing or future protocols. If the network is in the nature of a public network, such as the Internet, it may be advantageous to presume the network to be insecure and open to eavesdroppers. Specific information related to the protocols, standards, and application software utilized in connection with the Internet is generally known to those skilled in the art and, as such, need not be detailed herein. See, for example, Dilip Naik, Internet Standards and Protocols (1998); JAVA® 2 Complete, various authors, (Sybex 1999); Deborah Ray and Eric Ray, Mastering HTML 4.0 (1997); and Loshin, TCP/IP Clearly Explained (1997) and David Gourley and Brian Totty, HTTP, The Definitive Guide (2002).

[0057] The various system components may be independently, separately or collectively suitably coupled to the network via data links which includes, for example, a connection to an Internet Service Provider (ISP) over the local loop as is typically used in connection with standard modem communication, cable modem, Dish Networks®, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods, see, e.g., Gilbert Held, Understanding Data Communications (1996). It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network. Moreover, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

[0058] “Cloud” or “Cloud computing” includes a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing may include location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. For more information regarding cloud

computing, see the NIST's (National Institute of Standards and Technology) definition of cloud computing at <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (last visited June 2012),

5 [0059] The system and method may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the system may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the system may be implemented with any programming or scripting language such as C, C++, C#, JAVA®, JAVASCRIPT, VBScript, Macromedia Cold Fusion, COBOL, MICROSOFT® Active Server Pages, assembly, PERL, PHP, awk, Python, Visual Basic, SQL Stored Procedures, PL/SQL, any UNIX shell script, and extensible markup language (XML) with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the system may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the system could be used to detect or prevent security issues with a client-side scripting language, such as JAVASCRIPT, VBScript or the like. For a basic introduction of cryptography and network security, see any of the following references: (1) "Applied Cryptography: Protocols, Algorithms, And Source Code In C," by Bruce Schneier, published by John Wiley & Sons (second edition, 1995); (2) "JAVA® Cryptography" by Jonathan Knudson, published by O'Reilly & Associates (1998); (3) "Cryptography & Network Security: Principles & Practice" by William Stallings, published by Prentice Hall,

10
15
20
25

[0060] Each participant is equipped with a computing device in order to interact with the system and facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, cellular telephones, touch-tone telephones and the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are contemplated by the system. The bank has a computing center shown as a main frame computer. However, the bank

30

computing center may be implemented in other forms, such as a mini-computer, a PC server, a network of computers located in the same of different geographic locations, or the like. Moreover, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

5 [0061] As will be appreciated by one of ordinary skill in the art, the system may be embodied as a customization of an existing system, an add-on product, a processing apparatus executing upgraded software, a standalone system, a distributed system, a method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, any portion of the system or a module may take the form of a processing
10 apparatus executing code, an internet based embodiment, an entirely hardware embodiment, or an embodiment combining aspects of the internet, software and hardware. Furthermore, the system may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any suitable computer-readable storage medium may be utilized, including hard disks, CD-
15 ROM, optical storage devices, magnetic storage devices, and/or the like.

[0062] The system and method is described herein with reference to screen shots, block diagrams and flowchart illustrations of methods, apparatus (*e.g.*, systems), and computer program products according to various embodiments. It will be understood that each functional block of the block diagrams and the flowchart illustrations, and combinations of
20 functional blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions.

[0063] These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions that execute on the computer or other
25 programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks. These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction
30 means which implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such

that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

[0064] Accordingly, functional blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps
5 for performing the specified functions, and program instruction means for performing the specified functions. It will also be understood that each functional block of the block diagrams and flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, can be implemented by either special purpose hardware-based computer systems which perform the specified functions or steps, or suitable
10 combinations of special purpose hardware and computer instructions. Further, illustrations of the process flows and the descriptions thereof may make reference to user WINDOWS®, webpages, websites, web forms, prompts, etc. Practitioners will appreciate that the illustrated steps described herein may comprise in any number of configurations including the use of WINDOWS®, webpages, web forms, popup WINDOWS®, prompts and the like. It should
15 be further appreciated that the multiple steps as illustrated and described may be combined into single webpages and/or WINDOWS® but have been expanded for the sake of simplicity. In other cases, steps illustrated and described as single process steps may be separated into multiple webpages and/or WINDOWS® but have been combined for simplicity.

[0065] In yet another embodiment, payment application 102 is configured with a
20 biometric security system that may be used for providing biometrics as a secondary form of identification. The biometric security system may include a transponder and a reader communicating with the system. The biometric security system also may include a biometric sensor that detects biometric samples and a device for verifying biometric samples. The biometric security system may be configured with one or more biometric scanners,
25 processors and/or systems. A biometric system may include one or more technologies, or any portion thereof, such as, for example, recognition of a biometric. As used herein, a biometric may include a user's voice, fingerprint, facial, ear, signature, vascular patterns, DNA sampling, hand geometry, sound, olfactory, keystroke/typing, iris, retinal or any other biometric relating to recognition based upon any body part, function, system, attribute and/or
30 other characteristic, or any portion thereof.

[0066] The payment application 102 may include or interface with any of the foregoing devices and/or a transponder and reader (e.g. RFID reader) in RF communication with the transponder (which may include a fob), or communications between an initiator and a target

enabled by near field communications (NFC). Typical devices may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation. Moreover, the system, computing unit or device discussed herein may include a “pervasive computing device,” which may include a traditionally non-computerized device that is embedded with a computing unit. Examples may include watches, Internet enabled kitchen appliances, restaurant tables embedded with RF readers, wallets or purses with imbedded transponders, etc. Furthermore, a device or financial transaction instrument may have electronic and communications functionality enabled, for example, by: a network of electronic circuitry that is printed or otherwise incorporated onto or within the transaction instrument (and typically referred to as a “smart card”); a fob having a transponder and an RFID reader; and/or near field communication (NFC) technologies. For more information regarding NFC, refer to the following specifications;

ISO/IEC 18092 / ECMA-340, Near Field Communication Interface and Protocol-1 (NFCIP-1); ISO/IEC 21481 / ECMA-352, Near Field Communication Interface and Protocol-2 (NFCIP-2); and EMV 4.3 available at <http://www.emvco.com/default.aspx>.

[0067] Phrases and terms similar to “account”, “account number”, “account code” or “consumer account” as used herein, may include any device, code (e.g., one or more of an authorization/access code, personal identification number (“PIN”), Internet code, other identification code, and/or the like), number, letter, symbol, digital certificate, smart chip, digital signal, analog signal, biometric or other identifier/indicia suitably configured to allow the consumer to access, interact with or communicate with the system. The account number may optionally be located on or associated with a rewards account, charge account, credit account, debit account, prepaid account, telephone card, embossed card, smart card, magnetic stripe card, bar code card, transponder, radio frequency card or an associated account

[0068] The term “non-transitory” is to be understood to remove only propagating transitory signals per se from the claim scope and does not relinquish rights to all standard computer-readable media that are not only propagating transitory signals per se.

[0069] Benefits, other advantages, and solutions to problems have been described herein with regard to specific embodiments. However, the benefits, advantages, solutions to

problems, and any elements that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of the disclosure. The scope of the disclosure is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more." Moreover, where a phrase similar to 'at least one of A, B, and C' or 'at least one of A, B, or C' is used in the claims or specification, it is intended that the phrase be interpreted to mean that A alone may be present in an embodiment, B alone may be present in an embodiment, C alone may be present in an embodiment, or that any combination of the elements A, B and C may be present in a single embodiment; for example, A and B, A and C, B and C, or A and B and C.

[0070] Although the disclosure includes a method, it is contemplated that it may be embodied as computer program instructions on a tangible computer-readable carrier, such as a magnetic or optical memory or a magnetic or optical disk. All structural, chemical, and functional equivalents to the elements of the various embodiments that are known to those of ordinary skill in the art are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present disclosure, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. As used herein, the terms "comprises", "comprising", or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method comprising:

receiving, by a processor, an authentication MAC, an integrity MAC, and transaction data transmitted from a payment application and a payment terminal, wherein the integrity MAC is generated from the transaction data using a cryptography key stored in the payment application;

generating, by the processor, a local integrity MAC using the transaction data as an input to a first cryptographic operation using a copy of the cryptography key accessible by the processor;

determining, by the processor, that the received integrity MAC fails to match the local integrity MAC by comparing the local integrity MAC to the received integrity MAC;

retrieving, by the processor, an input to a second cryptographic operation, wherein the input to the second cryptographic operation is generated independently from the transaction data received by the processor from the payment application and the payment terminal;

generating, by the processor, a local authentication MAC using the second cryptographic operation;

in response to the received integrity MAC failing to match the local integrity MAC, authenticating, by the processor, the received authentication MAC by comparing, by the processor, the local authentication MAC to the received authentication MAC; and

in response to authenticating the received authentication MAC, authenticating, by the processor, the payment application.

2. The method of claim 1, wherein the input to the second cryptographic operation comprises data replicable at an issuer host.

3. The method of claim 1 or 2, wherein the first cryptographic operation is the same as the second cryptographic operation.

4. The method of claim 1 or 2, wherein the first cryptographic operation comprises an authentication encryption mode.

5. The method of any one of claims 1 to 4, further comprising approving a transaction in response to the successful authentication of at least one of the authentication MAC or the integrity MAC.

6. The method of any one of claims 1 to 5, wherein the authentication MAC and the integrity MAC are transmitted from the payment application, to the payment terminal, through a payment network, and to the processor.

7. A computer-based system comprising:
a processor;
a tangible, non-transitory memory configured to communicate with the processor, the tangible, non-transitory memory having instructions stored thereon that, in response to execution by the processor, cause the processor to perform operations comprising:
receiving, by the processor, an authentication MAC, an integrity MAC, and transaction data transmitted from a payment application and a payment terminal, wherein the integrity MAC is generated from the transaction data using a cryptography key stored in the payment application;
generating, by the processor, a local integrity MAC using the transaction data as an input to a first cryptographic operation using a copy of the cryptography key accessible by the processor;
determining, by the processor, that the received integrity MAC fails to match the local integrity MAC by comparing, by the processor, the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC;
retrieving, by the processor, an input to a second cryptographic operation, wherein the input to the second cryptographic operation is generated independently from the transaction

data received by the processor from the payment application and the payment terminal;
generating, by the processor, a local authentication MAC using the second
cryptographic operation;

in response to the received integrity MAC failing to match the local integrity MAC,
authenticating, by the processor, the received authentication MAC by comparing, by the
processor, the local authentication MAC to the received authentication MAC to authenticate
the received authentication MAC; and

in response to authenticating the received authentication MAC, authenticating, by
the processor, the payment application in response to a successful authentication of at
least one of the received authentication MAC or the received integrity MAC.

8. The computer-based system of claim 7, wherein the input to the second
cryptographic operation comprises data replicable at an issuer host.

9. The computer-based system of claim 7 or 8, wherein the first
cryptographic operation is the same as the second cryptographic operation.

10. The computer-based system of claim 7 or 8, wherein the first
cryptographic operation comprises an authentication encryption mode.

11. The computer-based system of any one of claims 7 to 10, further
comprising approving a transaction in response to the successful authentication of at
least one of the authentication MAC or the integrity MAC.

12. The computer-based system of any one of claims 7 to 11, wherein the
authentication MAC, the integrity MAC, and the transaction data are transmitted from
the payment application, to the payment terminal, through a payment network, and to
the processor.

13. An article of manufacture including a non-transitory, tangible computer readable storage medium having instructions stored thereon that, in response to execution by a processor, cause the processor to perform operations comprising:

receiving, by the processor, an authentication MAC, an integrity MAC, and transaction data transmitted from a payment application and a payment terminal, wherein the integrity MAC is generated from the transaction data using a cryptography key stored in the payment application;

generating, by the processor, a local integrity MAC using the transaction data as an input to a first cryptographic operation using a copy of the cryptography key accessible by the processor;

determining, by the processor, that the received integrity MAC fails to match the local integrity MAC by comparing, by the processor, the local integrity MAC to the received integrity MAC to authenticate the received integrity MAC;

retrieving, by the processor, an input to a second cryptographic operation, wherein the input to the second cryptographic operation is generated independently from the transaction data received by the processor from the payment application and the payment terminal;

generating, by the processor, a local authentication MAC using the second cryptographic operation;

in response to the received integrity MAC failing to match the local integrity MAC, authenticating, by the processor, the received authentication MAC by comparing, by the processor, the local authentication MAC to the received authentication MAC to authenticate the received authentication MAC; and

in response to authenticating the received authentication MAC, authenticating, by the processor, the payment application in response to a successful authentication of at least one of the received authentication MAC or the received integrity MAC.

14. The article of claim 13, wherein the input to the second cryptographic operation may comprise data replicable at an issuer host.

15. The article of claim 13 or 14, wherein the first cryptographic operation is the same as the second cryptographic operation.

16. The article of claim 13 or 14, wherein the first cryptographic operation comprises an authentication encryption mode.

17. The article of any one of claims 13 to 16, further comprising approving a transaction in response to the successful authentication of at least one of the authentication MAC or the integrity MAC.

100

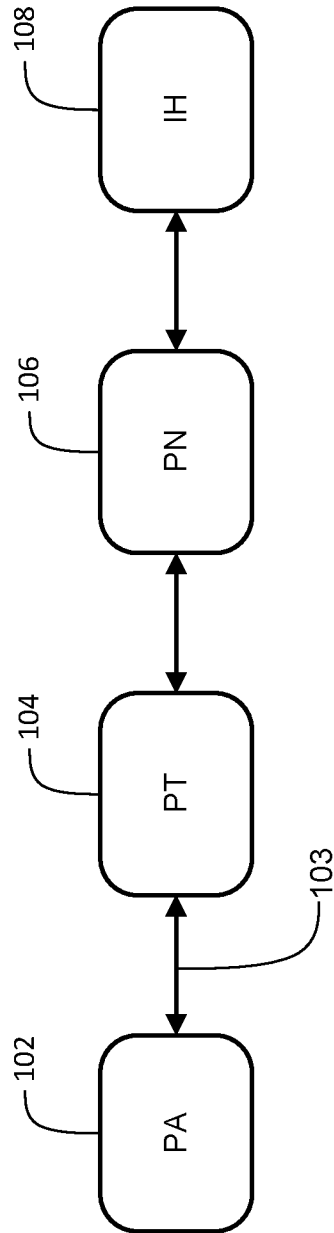


FIG. 1

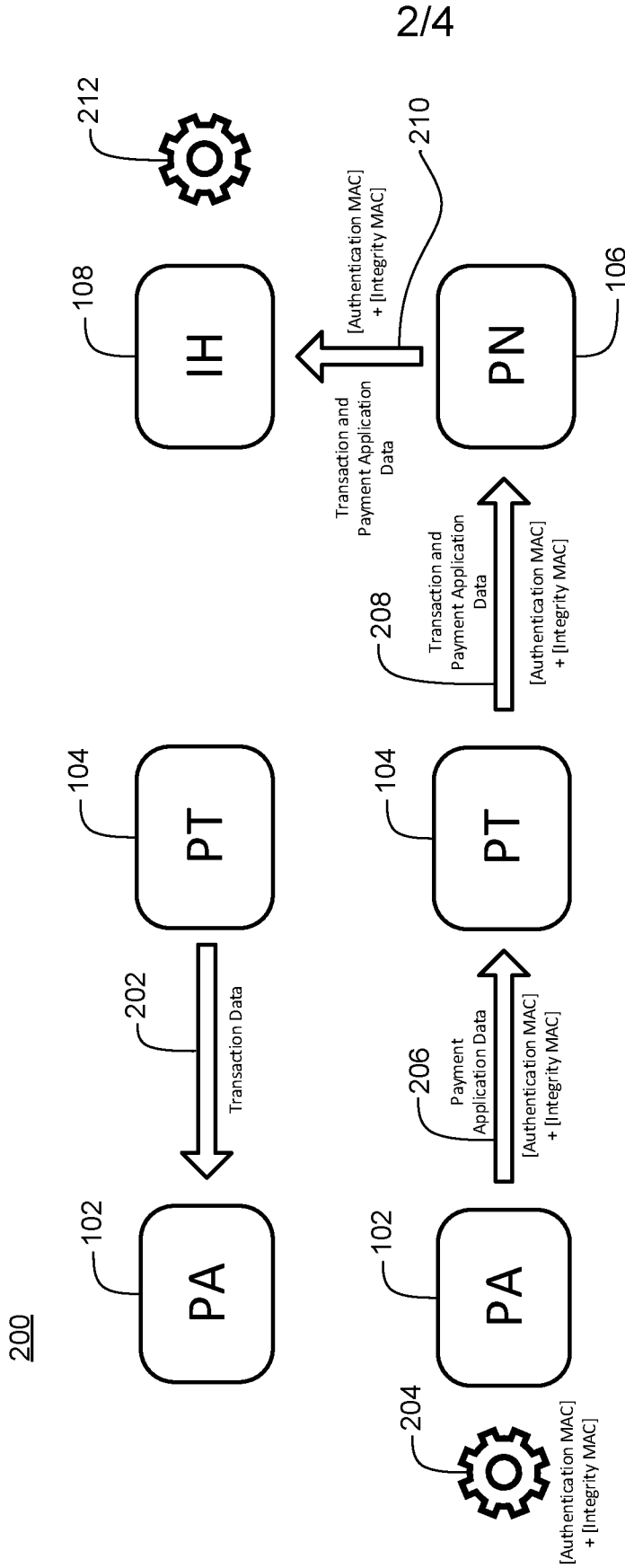


FIG. 2

3/4

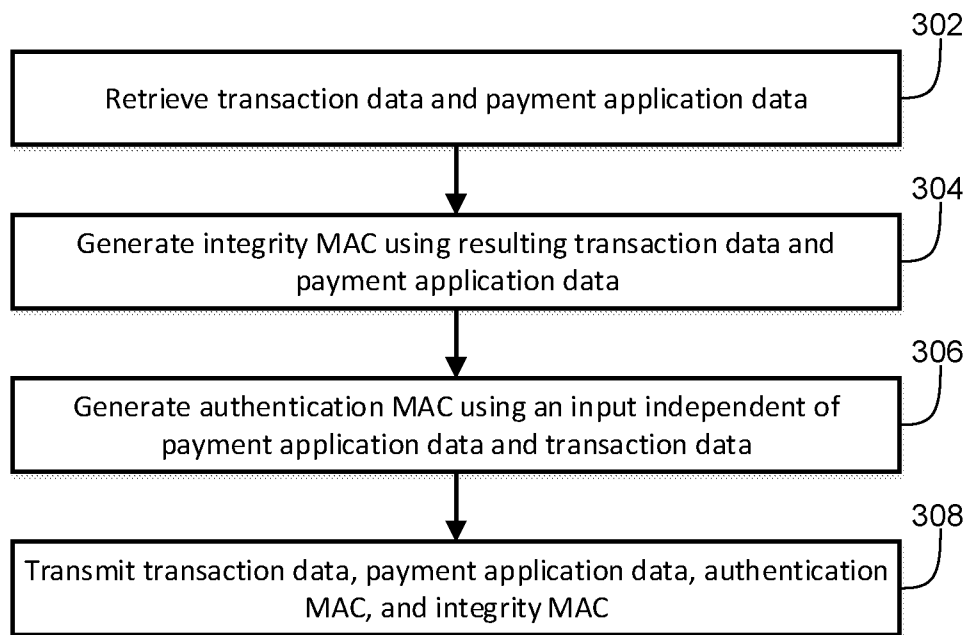
300

FIG. 3

4/4

400

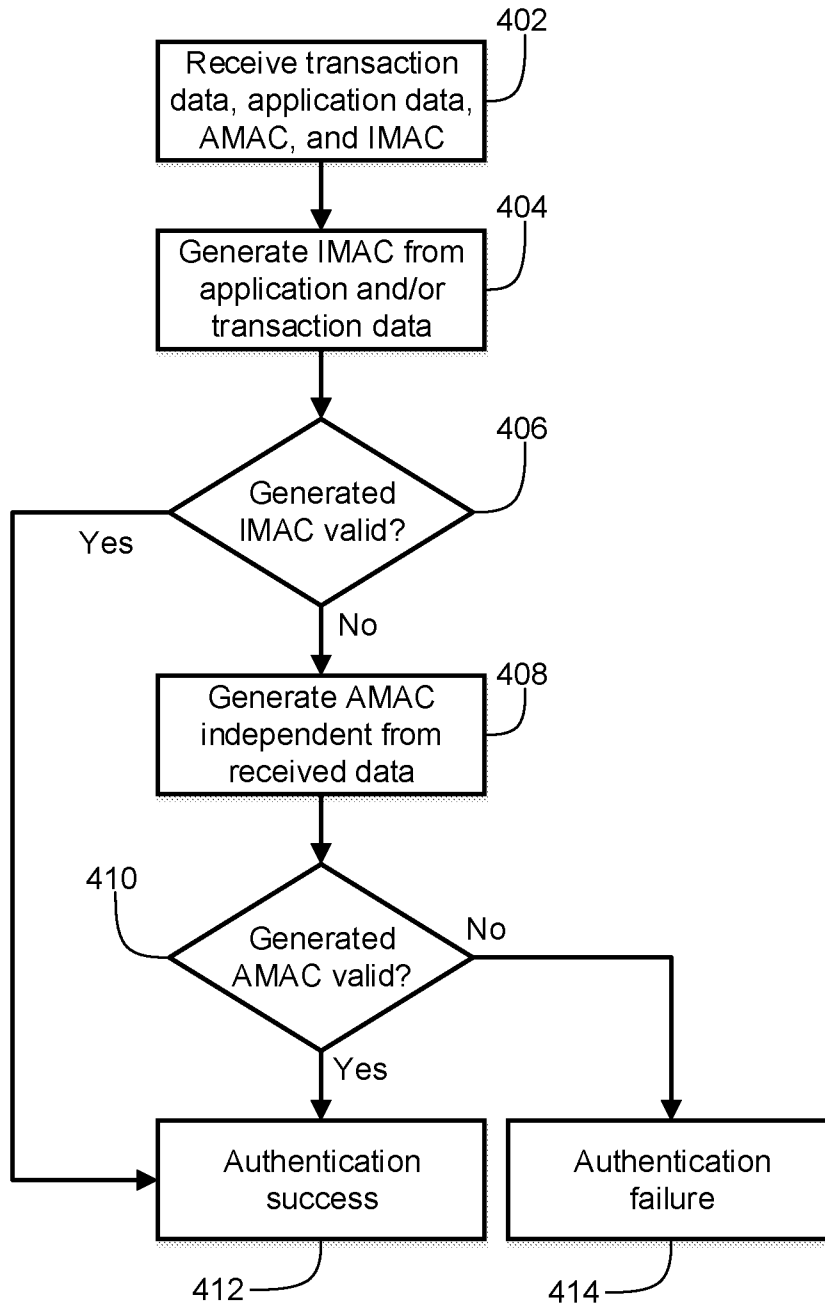


FIG. 4

